COMISIÓN
EUROPEA

Estrasburgo, 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Propuesta de

RECOMENDACIÓN DEL CONSEJO

sobre un enfoque coordinado de la Unión para reforzar la resiliencia de las infraestructuras críticas

(Texto pertinente a efectos del EEE)

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

La seguridad es un objetivo esencial de la Unión Europea. Si bien los Estados miembros tienen la responsabilidad primordial de proteger a los ciudadanos, la acción colectiva de toda la Unión contribuye en gran medida a la seguridad de la UE en su conjunto. La coordinación ayuda a reforzar la resiliencia, mejorar la vigilancia y fortalecer nuestra respuesta colectiva. En el contexto de la Unión de la Seguridad de la UE, se han dado pasos importantes para desarrollar capacidades y medios para la prevención, la detección y la respuesta rápida a muchas amenazas a la seguridad, y para unir a los agentes de los sectores público y privado en un esfuerzo común.

Equipar a la UE para hacer frente a la constante evolución del panorama de amenazas requiere una vigilancia y una adaptación constantes. La guerra de agresión rusa contra Ucrania ha traído consigo nuevos riesgos, a menudo combinados como una amenaza híbrida. Uno de estos riesgos es la interrupción de la prestación de servicios esenciales por las entidades que explotan infraestructuras críticas en Europa, algo que ha quedado todavía más patente con el aparente sabotaje de los gasoductos Nord Stream y otros incidentes recientes. La sociedad depende en gran medida de infraestructuras tanto físicas como digitales y la interrupción de los servicios esenciales, ya sea por ataques físicos convencionales o por ciberataques, o por una combinación de ambos, puede tener consecuencias graves para el bienestar de los ciudadanos, para nuestras economías y para la confianza en nuestros sistemas democráticos.

Otro objetivo clave de la UE es garantizar el buen funcionamiento del mercado interior, también en lo que se refiere a los servicios esenciales prestados por las entidades que explotan infraestructuras críticas. Por ello, la UE ya ha adoptado una serie de medidas para reducir sus puntos vulnerables y aumentar la resiliencia de las entidades críticas, tanto en lo que respecta a los riesgos cibernéticos como no cibernéticos.

Se requieren medidas urgentes para reforzar la capacidad de la Unión para hacer frente a posibles ataques contra infraestructuras críticas, principalmente en la propia UE, pero también, cuando proceda, en su vecindad inmediata.

La propuesta de Recomendación del Consejo tiene por objeto intensificar el apoyo de la UE para mejorar la resiliencia de las infraestructuras críticas, y garantizar una coordinación a escala de la Unión en lo que a preparación y respuesta se refiere. Su objetivo es maximizar y acelerar el trabajo de protección de aquellos activos, instalaciones y sistemas que son necesarios para el funcionamiento de la economía y para prestar servicios esenciales en el mercado interior de los que dependen los ciudadanos, así como mitigar el impacto de cualquier ataque garantizando la recuperación más rápida posible. Si bien todas estas infraestructuras deben protegerse, la prioridad actualmente son los sectores de la energía, la infraestructura digital, el transporte y el espacio, debido a su carácter especialmente horizontal para la sociedad y la economía, y a las evaluaciones de riesgos actuales.

La UE tiene un papel especial que desempeñar a la hora de garantizar la resiliencia de las infraestructuras que atraviesan las fronteras terrestres o marítimas y que afectan a los intereses de varios Estados miembros, o que se utilizan para prestar servicios esenciales transfronterizos. No obstante, las infraestructuras críticas importantes para varios Estados miembros pueden estar situadas en un solo Estado miembro o incluso fuera del territorio de un Estado miembro, por ejemplo, en el caso de cables submarinos o gasoductos. La identificación clara de las infraestructuras críticas y de las entidades que las explotan, así

como de los riesgos que las amenazan, y el compromiso colectivo para protegerlas redundan en interés de todos los Estados miembros y de la UE en su conjunto.

El Parlamento Europeo y el Consejo ya han alcanzado un acuerdo político para profundizar en el marco legislativo para la UE, a fin de contribuir a reforzar la resiliencia de las entidades que explotan infraestructuras críticas. En el verano de 2022 se alcanzaron acuerdos sobre la Directiva relativa a la resiliencia de las infraestructuras críticas («Directiva REC»)[1] y la Directiva revisada sobre la seguridad de las redes y sistemas de información («Directiva SRI 2»)[2]. Esto representará una importante intensificación de las capacidades en comparación con el marco legislativo vigente, la Directiva 2008/114/CE, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección («Directiva sobre las ICE»)[3] y la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión («Directiva SRI»)[4]. Se espera que la nueva legislación entre en vigor a finales de 2022 o principios de 2023, y los Estados miembros deben dar prioridad a su transposición y aplicación de acuerdo al Derecho de la Unión.

En estas circunstancias, y dada la posible urgencia de hacer frente a las amenazas derivadas de la guerra de agresión rusa contra Ucrania, las medidas esbozadas en la nueva legislación deberían, cuando sea posible y adecuado, anticiparse desde hoy. La intensificación de la cooperación mutua desde ahora, contribuiría también a generar el impulso necesario para una aplicación efectiva cuando la nueva legislación esté plenamente en vigor.

El resultado sería ir más allá de los marcos actuales, tanto en lo que se refiere a la profundidad de la acción como a la amplitud de los sectores cubiertos. La nueva Directiva REC presenta un nuevo marco de cooperación, así como las obligaciones para los Estados miembros y las entidades destinadas a reforzar la resiliencia física no cibernética frente a las amenazas naturales y de origen humano de dichas entidades que prestan servicios esenciales en el mercado interior, con once sectores seleccionados[5]. La Directiva SRI 2 establecerá una amplia cobertura sectorial de las obligaciones de ciberseguridad. Ello comprenderá un nuevo requisito para que los Estados miembros incluyan, cuando proceda, los cables submarinos en sus estrategias de ciberseguridad.

La legislación exige que la Comisión asuma un importante papel de coordinación. En virtud de la Directiva REC, la Comisión desempeña un papel de apoyo y facilitación, que debe llevarse a cabo con la ayuda y la participación del Grupo de Resiliencia de las Entidades Críticas establecido por dicha Directiva, y debería complementar las actividades de los Estados miembros mediante el desarrollo de mejores prácticas, material orientativo y metodologías. En cuanto a la ciberseguridad, el Consejo, en sus Conclusiones sobre la posición de la UE en materia de ciberseguridad del verano de 2022, ya ha invitado a la Comisión, al Alto Representante y al Grupo de cooperación SRI a trabajar sobre las evaluaciones de riesgos y los escenarios desde la perspectiva de la ciberseguridad. Dicha coordinación puede inspirar un enfoque para otras infraestructuras críticas clave.

---

1 COM(2020) 829 final.
2 COM(2020) 823 final.
3 DO L 345 de 23.12.2008.
4 DO L 194 de 19.7.2016.
5 Energía, transporte, infraestructura digital, banca, infraestructuras de los mercados financieros, sanidad, agua potable, aguas residuales, administraciones públicas, espacio y alimentación.

El 5 de octubre de 2022, la presidenta Von der Leyen presentó un plan de cinco puntos que establece un planteamiento coordinado de la labor necesaria para el futuro. Sus elementos clave fueron los siguientes: mejorar la preparación; trabajar con los Estados miembros para probar la resistencia de sus infraestructuras críticas, empezando por el sector de la energía y continuando con otros sectores de alto riesgo; aumentar la capacidad de respuesta, en particular, a través del Mecanismo de Protección Civil de la Unión; hacer un buen uso de la capacidad satelital para detectar posibles amenazas; y fortalecer la cooperación con la Organización del Tratado del Atlántico Norte (OTAN) y con socios clave en materia de resiliencia de las infraestructuras críticas. El plan de cinco puntos subrayaba el valor de anticipar la legislación para la que ya existe un acuerdo político.

La propuesta de Recomendación del Consejo acoge con satisfacción este enfoque para estructurar el apoyo de los Estados miembros y coordinar sus esfuerzos por crear una mayor sensibilización sobre los riesgos y mejorar la preparación y la respuesta a las amenazas actuales. A este respecto, se convocan reuniones de expertos para debatir la resiliencia de las entidades que explotan infraestructuras críticas en anticipación a la entrada en vigor de la Directiva REC y del Grupo de Resiliencia de las Entidades Críticas que dicha Directiva establece.

El refuerzo de la cooperación con socios clave y países vecinos y con otros terceros países pertinentes sobre la resiliencia de las entidades que explotan infraestructuras críticas será esencial, en particular a través del diálogo estructurado UE-OTAN en materia de resiliencia.

La presente Recomendación se centra en el refuerzo de la capacidad de la Unión para anticiparse, prevenir y responder a las nuevas amenazas derivadas de la guerra de agresión rusa contra Ucrania. Por lo tanto, las recomendaciones propuestas se centran en abordar los riesgos y amenazas relacionados con la seguridad de las infraestructuras críticas. No obstante, cabe señalar que los acontecimientos recientes también han puesto de relieve la acuciante necesidad de prestar más atención a los efectos del cambio climático en las infraestructuras y servicios críticos, por ejemplo, en lo referente a los suministros de agua para la refrigeración de las centrales nucleares, las centrales hidroeléctricas y la navegación interior, que se ven comprometidos y son impredecibles según las estaciones, o el riesgo de daños materiales a las infraestructuras de transporte, que pueden causar perturbaciones importantes en los servicios esenciales. Estas inquietudes se seguirán abordando mediante la legislación y la coordinación pertinentes.

- **Coherencia con las disposiciones existentes en la misma política sectorial**

La presente propuesta de Recomendación del Consejo está plenamente en consonancia con el marco jurídico futuro sobre la resiliencia de las entidades que explotan infraestructuras críticas en la UE, la Directiva sobre las ICE y la Directiva REC respectivamente, ya que tiene por objeto, entre otras cosas, facilitar la cooperación entre los Estados miembros en este ámbito y respaldar medidas concretas para mejorar la resiliencia frente a las amenazas inminentes actuales contra las entidades que explotan infraestructuras críticas en la UE.

Asimismo, completa y anticipa la Directiva REC invitando ya a los Estados miembros a dar prioridad a la oportuna trasposición de la Directiva, cooperando mediante reuniones de expertos convocadas como parte del plan de cinco puntos anunciado por la Comisión y tratando de coordinar el camino hacia un enfoque común para la realización de pruebas de resistencia en infraestructuras críticas de la UE.

La propuesta también está en consonancia con la Directiva SRI y la futura Directiva SRI 2, que derogará la Directiva SRI, al pedir un comienzo temprano de la labor de aplicación y transposición. También refleja el llamamiento conjunto de Nevers, de marzo de 2022, así

como las Conclusiones del Consejo sobre la posición de la UE en materia de ciberseguridad, de mayo de 2022, en lo relativo a la petición de los Estados miembros a la Comisión de que desarrolle evaluaciones del riesgo y escenarios de riesgo.

Asimismo, la propuesta está en consonancia con la política de la UE sobre protección civil, según la cual, en caso de una perturbación en las operaciones de las infraestructuras o entidades críticas, los Estados miembros y terceros países pueden solicitar asistencia a través del Centro de Coordinación de la Respuesta a Emergencias (CECRE) en el marco del Mecanismo de Protección Civil de la Unión (MPCU). En caso de activación del MPCU, el CECRE puede coordinar y cofinanciar el despliegue en el país afectado de los equipos esenciales, el material y los conocimientos especializados disponibles en los Estados miembros (en parte en el contexto de la Reserva Europea de Protección Civil) y en el marco de rescEU. La asistencia, que puede facilitarse previa solicitud, incluye, por ejemplo, combustible, generadores, infraestructura eléctrica, capacidad de alojamiento, equipos de purificación de agua y asistencia médica de emergencia.

La propuesta también está en consonancia con el acervo de la UE relativo a la seguridad del abastecimiento energético.

El sector de la energía nuclear no está incluido específicamente en la propuesta de Recomendación del Consejo, excepto, por ejemplo, las infraestructuras conexas (como las líneas de transmisión a las centrales nucleares) que puedan afectar a la seguridad del suministro. Los elementos nucleares específicos están cubiertos por la correspondiente legislación en materia nuclear en virtud del Tratado Euratom o de la legislación nacional[6]. Sobre la base de la experiencia adquirida tras el accidente de Fukushima, se reforzó la legislación europea en materia de seguridad nuclear y, por ello, las autoridades nacionales deben llevar a cabo revisiones de seguridad periódicas para cada instalación a fin de garantizar el cumplimiento continuado de los requisitos de seguridad más elevados y determinar nuevas mejoras en materia de seguridad, y deben realizarse revisiones temáticas por homólogos cada seis años a escala de la UE.

La Estrategia de Seguridad Marítima de la Unión Europea[7] y su plan de acción[8] destacan la naturaleza cambiante de las amenazas en el ámbito marítimo y piden un compromiso renovado con la protección de las infraestructuras marítimas críticas, también las submarinas, y en particular del transporte marítimo y las infraestructuras de energía y comunicación, entre otras cosas, mediante un mejor conocimiento del ámbito marítimo, a través de la mejora de la interoperabilidad y la racionalización del intercambio de información.

La propuesta también está en consonancia con otra legislación sectorial pertinente. Por lo tanto, la aplicación de la presente Recomendación debe ser coherente con las medidas específicas que regulan o puedan regular en el futuro determinados aspectos de la resiliencia de las entidades que operan en sectores afectados como el transporte. Esto incluye otras iniciativas pertinentes como el plan de contingencia para el transporte[9] o el plan de contingencia para garantizar el suministro de alimentos y la seguridad alimentaria en tiempos de crisis[10] y el Mecanismo Europeo de Preparación y Respuesta ante las Crisis de Seguridad Alimentaria. De forma más general, la Recomendación debe, naturalmente, ejecutarse

6 Considerando 9 de la Directiva 2008/114/CE del Consejo (Directiva sobre las ICE).
7 Ref. 11205/14.
8 Ref. 10494/18.
9 COM(2022) 211.
10 COM(2021) 689.

respetando plenamente todas las normas aplicables del Derecho de la Unión, incluidas las establecidas en la Directiva sobre las ICE y la Directiva SRI.

La propuesta también está en línea con la Brújula Estratégica para la Seguridad y la Defensa, que puso de relieve la necesidad de mejorar sustancialmente la resiliencia y la capacidad para hacer frente a amenazas híbridas y ciberataques, así como la necesidad de fortalecer la resiliencia de países socios y de cooperar con la OTAN. Está también en consonancia con el marco para una respuesta coordinada de la UE a las campañas y amenazas híbridas que afectan a la Unión, a los Estados miembros y a países socios[11].

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

La propuesta se basa en el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), que implica la aproximación de la legislación para la mejora del mercado interior, y en el artículo 292 del TFUE. Esto se justifica por el hecho de que la propuesta de Recomendación del Consejo busca principalmente anticipar las medidas establecidas en las nuevas Directivas REC y SRI 2, que también se basan en el artículo 114 del TFUE. En consonancia con la lógica que justifica el uso de dicho artículo como base jurídica para estas Directivas, es necesaria la actuación de la UE para garantizar el buen funcionamiento del mercado interior, en particular, teniendo en cuenta la naturaleza y el alcance transfronterizos de los servicios en cuestión y las posibles consecuencias en caso de interrupciones de dichos servicios, así como las medidas nacionales existentes y futuras destinadas a aumentar la resiliencia de las entidades que explotan las infraestructuras críticas utilizadas para prestar servicios esenciales en el mercado interior.

• Subsidiariedad (en el caso de competencia no exclusiva)

Una acción para el futuro a escala europea en el ámbito de la resiliencia de las entidades que explotan infraestructuras críticas está justificada por la interdependencia y el carácter transfronterizo de las relaciones entre el funcionamiento de infraestructuras críticas y los servicios esenciales prestados, y por la necesidad de un enfoque europeo más común y coordinado, para garantizar que las entidades en cuestión sean suficientemente resilientes en el actual contexto geopolítico. Si bien, muchos de los retos comunes, como el aparente sabotaje de los gasoductos Nord Stream, se abordan principalmente a través de medidas nacionales o por parte de las entidades que explotan infraestructuras críticas, el apoyo de la UE, incluidas las agencias pertinentes cuando proceda, será necesario para fortalecer la resiliencia, mejorar la vigilancia y reforzar la respuesta colectiva de la UE.

• Proporcionalidad

La presente propuesta se ajusta al principio de proporcionalidad establecido en el artículo 5, apartado 4, del Tratado de la Unión Europea (TUE).

Ni el contenido ni la forma de esta propuesta de Recomendación del Consejo exceden de lo necesario para alcanzar sus objetivos. Las medidas propuestas son proporcionales a los objetivos perseguidos, ya que respetan las prerrogativas y obligaciones de los Estados miembros en virtud del Derecho nacional.

[11] Consejo de la Unión Europea, ref. 10016/22, de 21 de junio de 2022.

Finalmente, la propuesta incorpora un posible enfoque diferenciado que refleja las diversas realidades internas de los Estados miembros en lo que respecta a la preparación y la respuesta a las amenazas físicas a las infraestructuras.

- **Elección del instrumento**

Para alcanzar los objetivos mencionados, el TFUE, en particular en su artículo 292, prevé que el Consejo adopte recomendaciones basadas en una propuesta de la Comisión. Una recomendación del Consejo es un instrumento adecuado en este caso, teniendo en cuenta también el contexto legislativo actual, como se ha explicado anteriormente. Como acto jurídico, aunque de carácter no vinculante, una recomendación del Consejo señala el compromiso de los Estados miembros con las medidas incluidas y proporciona una sólida base política para la cooperación en estos ámbitos, respetando plenamente la autoridad de los Estados miembros.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- **Consultas con las partes interesadas**

Al elaborar la presente propuesta se han tenido en cuenta las opiniones expresadas por los expertos en la reunión del 12 de octubre de 2022. Hubo un amplio consenso sobre la conveniencia de una mayor coordinación a escala de la Unión en lo que respecta a la preparación y la respuesta en el contexto actual de amenazas y para anticipar determinados elementos de la Directiva REC antes de su adopción formal. Los Estados miembros se mostraron dispuestos a compartir experiencias y mejores prácticas sobre las medidas y metodologías necesarias para mejorar la resiliencia de las entidades que explotan infraestructuras críticas. También expresaron su disposición a adoptar un enfoque común para probar la resistencia de las entidades que explotan infraestructuras de forma voluntaria y sobre la base de principios comunes. Los Estados miembros indicaron que las entidades que explotan infraestructuras críticas en los sectores de la energía, la infraestructura digital y el transporte deben considerarse prioritarias a efectos de la presente Recomendación, en particular, las que sean más importantes para algunos Estados miembros. También acogieron con satisfacción la intención de la Comisión de convocar nuevas reuniones de expertos de los Estados miembros en las próximas semanas.

- **Explicación detallada de las disposiciones específicas de la propuesta**

La propuesta de Recomendación del Consejo establece lo siguiente:

– El capítulo I establece el objetivo de la propuesta, indicando qué abarca y la determinación de prioridades entre las medidas recomendadas.

– El capítulo II se centra en las medidas que deben adoptarse para mejorar la preparación, tanto a escala de la Unión como de los Estados miembros.

– El capítulo III analiza la respuesta reforzada, tanto a escala de la UE como de los Estados miembros.

– El capítulo IV se ocupa de la cooperación internacional y de las medidas que deben adoptarse para aumentar la resiliencia de las entidades que explotan infraestructuras críticas.

2022/0338 (NLE)

Propuesta de

RECOMENDACIÓN DEL CONSEJO

sobre un enfoque coordinado de la Unión para reforzar la resiliencia de las infraestructuras críticas

(Texto pertinente a efectos del EEE)

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular sus artículos 114 y 292,

Vista la propuesta de la Comisión Europea,

Considerando lo siguiente:

(1) La Unión tiene un papel especial que desempeñar en relación con las infraestructuras que atraviesan fronteras y que afectan a los intereses de varios Estados o que son utilizadas de otro modo por entidades para prestar servicios esenciales a escala transfronteriza. No obstante, la prestación de servicios y las infraestructuras críticas que son importantes para varios Estados miembros pueden estar situadas en un Estado miembro o fuera del territorio de los Estados miembros, por ejemplo, en el caso de cables submarinos o gasoductos. La identificación clara de dichas infraestructuras y entidades y de las amenazas a las que se enfrentan, así como el compromiso colectivo de protegerlas, redunda en interés de todos los Estados miembros y de la Unión en su conjunto.

(2) La protección de las infraestructuras críticas en dos sectores está actualmente regulada por la Directiva 2008/114/CE del Consejo[12] Dicha Directiva establece un procedimiento de identificación y designación de infraestructuras críticas europeas y un planteamiento común para evaluar la necesidad de mejorar la protección de dichas infraestructuras, con el fin de contribuir a la protección de la población. Cubre los sectores de la energía y el transporte. A fin de mejorar la resiliencia de las entidades críticas y los servicios esenciales que prestan y de las infraestructuras críticas de las que dependen, está en proceso de adopción por el legislador de la Unión una nueva Directiva sobre la resiliencia de las entidades críticas[13] (la «Directiva REC»), que sustituirá a la Directiva 2008/114/CE, cubriendo más sectores, como la infraestructura digital.

(3) Además, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes

[12] Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (DO L 345 de 23.12.2008, p. 75).

[13] COM(2020) 829.

y sistemas de información en la Unión[14] se centra en las amenazas relacionadas con la ciberseguridad. Esta Directiva será sustituida por una nueva Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión[15] («Directiva SRI 2»), que también está en proceso de adopción por el legislador de la Unión.

(4) En vista de la rápida evolución del panorama de amenazas, en particular en el contexto del aparente sabotaje de la infraestructura de gas Nord Stream 1 y 2, las entidades que explotan infraestructuras críticas se enfrentan a retos particulares en lo que se refiere a su resiliencia frente a actos hostiles y otras amenazas de origen humano, mientras que los retos derivados de factores naturales y del cambio climático están aumentando y pueden interactuar con los actos hostiles. Por lo tanto, deben adoptar, con el apoyo de los Estados miembros, medidas adecuadas de mejora de la resiliencia. Las medidas y el apoyo deben adoptarse y prestarse más allá de las medidas recogidas en la Directiva 2008/114/CE y en la Directiva (UE) 2016/1148, e incluso antes de la adopción, entrada en vigor y trasposición de las nuevas Directivas REC y SRI 2.

(5) A la espera de la adopción, entrada en vigor y transposición de estas nuevas Directivas, se anima a la Unión y a los Estados miembros, de conformidad con el Derecho de la Unión, a utilizar todas las herramientas disponibles para avanzar y ayudar a reforzar la resiliencia física y cibernética de dichas entidades y de las infraestructuras críticas que explotan para prestar servicios esenciales en el mercado interior, es decir, servicios que son fundamentales para mantener las funciones sociales vitales, las actividades económicas, la salud y la seguridad públicas o para el medio ambiente. A este respecto, el concepto de resiliencia debe entenderse como la capacidad de una entidad para prevenir, proteger, responder, resistir, mitigar, absorber, adaptarse y recuperarse de acontecimientos que perturben o puedan perturbar de forma significativa la prestación de los servicios esenciales en cuestión.

(6) A fin de garantizar un enfoque que sea a la vez eficaz y lo más coherente posible con la nueva Directiva REC, las medidas contenidas en la presente Recomendación deben referirse a las infraestructuras designadas por un Estado miembro como infraestructuras críticas, lo que incluye tanto infraestructuras críticas nacionales como europeas, con independencia de que la entidad que explote la infraestructura crítica haya sido designada como entidad crítica en virtud de esa nueva Directiva. A efectos de la presente Recomendación, el término «infraestructura crítica» debe entenderse en consecuencia.

(7) En vista de las amenazas existentes, deben adoptarse con carácter prioritario medidas de mejora de la resiliencia en los sectores clave de la energía, la infraestructura digital, el transporte y el espacio, y dichas medidas deben centrarse en aumentar la resiliencia de las entidades que explotan infraestructuras críticas frente a los riesgos provocados por el hombre. En lo que respecta a las infraestructuras críticas nacionales, habida cuenta de las posibles consecuencias si se materializan los riesgos, debe darse prioridad a las infraestructuras de importancia transfronteriza.

(8) En consecuencia, las medidas establecidas en la presente Recomendación tienen como objetivo principal completar las nuevas Directivas REC y SRI 2, que se basan en el

[14] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).

[15] COM(2020) 823.

artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), anticipando y complementando las medidas que estas nuevas Directivas ofrecerán. Por lo tanto, en vista del carácter transfronterizo y la importancia de los servicios esenciales y las infraestructuras críticas en cuestión, y de las actuales y futuras disparidades de las legislaciones nacionales que distorsionan el mercado interior, procede basar también la presente Recomendación en el artículo 114 del TFUE, junto con el artículo 292 del TFUE.

(9) La aplicación de la presente Recomendación no debe entenderse de manera que afecte a los requisitos actuales y futuros del Derecho de la Unión relativos a determinados aspectos de la resiliencia de las entidades afectadas y debe ser coherente con ellos. Dichos requisitos se establecen en instrumentos generales como la Directiva 2008/114/CE y la Directiva (UE) 2016/1148 y las nuevas Directivas REC y SRI 2 que las sustituyen, pero también en determinados instrumentos sectoriales como en el ámbito del transporte, en el que, entre otras cosas, la Comisión ha adoptado una iniciativa sobre un plan de contingencia para el transporte[16]. De conformidad con el principio de cooperación leal, la presente Recomendación debe aplicarse con pleno respeto y asistencia mutuos.

(10) El 5 de octubre de 2022, la Comisión anunció un plan de cinco puntos en el que se establece un enfoque coordinado para hacer frente a los retos futuros, lo que supone trabajar en materia de preparación basándose en la nueva Directiva REC y anticipándose a su adopción y entrada en vigor, y supone también trabajar con los Estados miembros con vistas a la realización de pruebas de resistencia de las entidades que explotan infraestructuras críticas basadas en principios comunes, empezando por el sector de la energía. La presente Recomendación, que contribuirá a dicho plan, acoge con satisfacción el enfoque propuesto y establece cómo puede traducirse en acciones concretas.

(11) En el contexto de un panorama de amenazas en rápida evolución y del actual entorno de riesgo caracterizado por riesgos de origen humano, en particular en lo que se refiere a las infraestructuras críticas con relevancia transfronteriza, es esencial disponer de una imagen precisa, actualizada y completa de los riesgos más importantes a los que se enfrentan las entidades que explotan las infraestructuras críticas. Por lo tanto, los Estados miembros deben adoptar las medidas necesarias para llevar a cabo sus evaluaciones de dichos riesgos. Si bien la presente Recomendación se centra en los riesgos relacionados con la seguridad, también deben proseguir los esfuerzos para abordar los riesgos medioambientales y los relacionados con el cambio climático, en particular cuando los fenómenos naturales puedan exacerbar los riesgos provocados por el hombre.

(12) Teniendo en cuenta este panorama de amenazas, debe invitarse a los Estados miembros a adoptar lo antes posible medidas adecuadas para mejorar la resiliencia de las infraestructuras críticas, más allá de las mencionadas evaluaciones de riesgos, que posteriormente serán un requisito en virtud de la nueva Directiva REC.

(13) Como parte de la aplicación del plan de cinco puntos anunciado por la Comisión, es preciso coordinar el trabajo reuniendo a expertos nacionales en anticipación de la creación, en virtud de la Directiva REC, del Grupo de Resiliencia de las Entidades Críticas, a fin de posibilitar la cooperación entre los Estados miembros y el intercambio de información relativa a la resiliencia de las entidades que explotan

[16] COM(2022) 211.

infraestructuras críticas. Esto debe incluir la cooperación y el intercambio de información sobre actividades como la determinación de las entidades e infraestructuras críticas, la preparación del desarrollo y la promoción de un conjunto común de principios para realizar pruebas de resistencia y el aprendizaje de lecciones comunes a partir de dichas pruebas, identificando los puntos vulnerables y las posibles capacidades. Estos procesos también deberían beneficiar a la resiliencia de las entidades que explotan infraestructuras críticas frente a los riesgos climáticos y medioambientales. Esta labor permitiría además establecer prioridades comunes en la realización de pruebas de resistencia, con un énfasis en los sectores de la energía, la infraestructura digital, el transporte y el espacio. La Comisión ya ha comenzado a convocar a estos expertos y a facilitar su trabajo, y tiene la intención de proseguir esta labor. Una vez que la nueva Directiva REC haya entrado en vigor y se haya creado el Grupo de Resiliencia de las Entidades Criticas, este grupo debe proseguir este trabajo anticipatorio de conformidad con sus funciones en virtud de la Directiva REC.

(14) El ejercicio de realización de pruebas de resistencia debe completarse con la elaboración de un plan rector sobre incidentes y crisis en las infraestructuras críticas que describa y establezca los objetivos y modos de cooperación entre los Estados miembros y las instituciones, órganos, oficinas y agencias de la UE en respuesta a incidentes en las infraestructuras críticas, en particular cuando estos impliquen perturbaciones significativas de la prestación de servicios esenciales para el mercado interior. El plan rector debe hacer uso del Dispositivo de Respuesta Política Integrada a las Crisis (Dispositivo RPIC) para la coordinación de la respuesta a nivel normativo de la Unión, debe trabajar de forma coherente y complementaria con el plan rector sobre incidentes de ciberseguridad a gran escala, y debe, asimismo, prever un acuerdo sobre mensajes clave de comunicación al público, dado que la comunicación de las crisis desempeña un papel importante a la hora de mitigar los efectos negativos de los incidentes y las crisis en las infraestructuras críticas.

(15) A fin de garantizar una respuesta coordinada y eficaz a las amenazas actuales y previstas, la Comisión prestará apoyo adicional a los Estados miembros con vistas a mejorar la resiliencia a la luz de dichas amenazas, en particular facilitando información pertinente en forma de sesiones informativas, manuales y directrices, promoviendo la adopción de proyectos de investigación e innovación financiados por la Unión, adoptando las medidas anticipatorias necesarias y optimizando el uso de los medios de vigilancia de la Unión. El Servicio Europeo de Acción Exterior (SEAE) a través del Centro de Inteligencia y de Situación de la UE debe proporcionar evaluaciones de las amenazas.

(16) Las agencias de la Unión correspondientes a cada sector y otros organismos pertinentes también deben prestar apoyo en cuestiones relacionadas con la resiliencia, en la medida en que lo permitan sus respectivos mandatos recogidos en los correspondientes instrumentos del Derecho de la Unión. En particular, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) podría contribuir en cuestiones de ciberseguridad, la Agencia Europea de Seguridad Marítima (AESM) podría ayudar a los Estados miembros con sus conocimientos a través de su servicio de vigilancia marítima en asuntos relacionados con la seguridad y la protección marítimas, la Agencia de la Unión Europea para la Cooperación Policial (Europol) podría prestar apoyo en relación con la recopilación de información y las investigaciones en las acciones policiales transfronterizas, mientras que la Agencia de la Unión Europea para el Programa Espacial (EUSPA) y el Centro de Satélites de la Unión Europea (Satcen)

pueden prestar asistencia a través de operaciones en el marco del Programa Espacial de la Unión.

(17) Si bien la responsabilidad principal de garantizar la seguridad de las infraestructuras y las entidades críticas afectadas corresponde a los Estados miembros, una mayor coordinación a escala de la Unión es adecuada especialmente a la luz de amenazas que pueden afectar a varios Estados miembros a la vez, como la guerra de agresión rusa contra Ucrania, o afectar a la resiliencia y el buen funcionamiento de la economía, el mercado único y las sociedades de la Unión.

(18) La presente Recomendación no implica facilitar información cuya divulgación sea contraria a los intereses esenciales de los Estados miembros en materia de seguridad nacional, seguridad pública o defensa.

(19) Con la creciente interdependencia de las infraestructuras físicas y digitales, las actividades informáticas malintencionadas dirigidas a zonas críticas pueden dar lugar a perturbaciones o daños en las infraestructuras físicas, mientras que el sabotaje de infraestructuras físicas puede hacer que los servicios digitales queden inaccesibles. En vista de la amenaza cada vez mayor que suponen los sofisticados ataques híbridos, los Estados miembros deberían incluir también estas consideraciones en su labor de aplicación de la presente Recomendación. Habida cuenta de las interrelaciones entre la ciberseguridad y la seguridad física de los operadores, es importante que la labor de preparación para la transposición y aplicación de la nueva Directiva SRI 2 comience lo antes posible y dicha labor avance también en paralelo en virtud de la Directiva REC.

(20) Además de mejorar la preparación, es importante mejorar las capacidades para responder con rapidez y eficacia en el caso de que se materialicen los riesgos que afectan a la prestación servicios esenciales por parte de las entidades que explotan infraestructuras críticas. Por lo tanto, la presente Recomendación debe contener las medidas que deben adoptarse tanto a escala de los Estados miembros como de la Unión, incluida la cooperación reforzada y el intercambio de información en el contexto del Mecanismo de Protección Civil de la Unión y el uso de los recursos pertinentes del Programa Espacial de la Unión.

(21) Tras la invitación del Consejo en sus Conclusiones sobre la posición de la UE en materia de ciberseguridad[17], la Comisión, el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad (el «Alto Representante») y el Grupo de cooperación establecido por la Directiva (UE) 2016/1148 («Grupo de cooperación SRI»), en coordinación con los organismos y agencias civiles y militares pertinentes y las redes establecidas, como la red de organizaciones de enlace nacionales para la gestión de cibercrisis (CyCLONe), están llevando a cabo una evaluación de riesgos y elaborando escenarios de riesgo desde la perspectiva de la ciberseguridad en una situación de amenaza o posible ataque contra los Estados miembros o países socios. Este ejercicio se centra en sectores críticos como la energía, la infraestructura digital, el transporte y el espacio.

(22) El llamamiento ministerial conjunto de Nevers[18] y las Conclusiones del Consejo sobre la posición de la UE en materia de ciberseguridad instaban también a reforzar la resiliencia de las infraestructuras y redes de comunicaciones en la Unión, formulando

[17] *Cyber posture: Council approves conclusions - Consilium (europa.eu)* [«Posición sobre ciberseguridad: el Consejo aprueba las conclusiones», comunicado de prensa en inglés].

[18] https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf.

recomendaciones para los Estados miembros y la Comisión sobre la base de una evaluación de riesgos. Esta evaluación de riesgos está siendo realizada actualmente por el Grupo de cooperación SRI, con el apoyo de la Comisión y de la ENISA, y en colaboración con el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE). La evaluación de riesgos y el análisis de las deficiencias examina los riesgos de ciberataques con respecto a los distintos subsectores de las infraestructuras, entre ellas, las infraestructuras fijas y móviles, los satélites, los cables submarinos, el encaminamiento en internet, etc., proporcionando así una base para el trabajo con arreglo a la presente Recomendación. Esta evaluación de riesgos aportará información a la evaluación de riesgos cibernéticos intersectoriales en curso y a los escenarios solicitados por el Consejo en las Conclusiones del Conclusiones del Consejo de 23 de mayo de 2022.

(23) Estos dos ejercicios serán coherentes y estarán coordinados con el ejercicio de determinación de escenarios que se centra en la protección civil en el contexto de una amplia gama de catástrofes naturales y de origen humano, como acontecimientos de ciberseguridad y su impacto en la vida real, que actualmente están desarrollando la Comisión y los Estados miembros en virtud de la Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo[19]. En interés de la eficiencia, la eficacia y la coherencia, la presente Recomendación debe aplicarse teniendo en cuenta los resultados de dichos ejercicios.

(24) El conjunto de instrumentos de la UE sobre ciberseguridad de las redes 5G[20] establece medidas y planes de mitigación pertinentes para reforzar la seguridad de estas redes. Teniendo en cuenta la dependencia de las redes 5G que afecta a muchos servicios esenciales y el carácter interconectado de los ecosistemas digitales, es fundamental que todos los Estados miembros logren con urgencia la aplicación de las medidas recomendadas en el conjunto de herramientas y en particular apliquen las restricciones pertinentes a los proveedores de alto riesgo para activos clave definidos como críticos y sensibles en la evaluación de riesgos coordinada de la UE.

(25) Con el fin de reforzar de forma inmediata la preparación y las capacidades para responder a incidentes cibernéticos graves, la Comisión ha establecido un programa a corto plazo para apoyar a los Estados miembros mediante financiación adicional asignada a la ENISA. Los servicios cubiertos incluirán actividades de preparación como pruebas de penetración de las entidades críticas con el fin de detectar sus puntos vulnerables. El programa también reforzará las posibilidades de asistencia a los Estados miembros en caso de un incidente grave que afecte a entidades críticas. Se trata de un primer paso en consonancia con las Conclusiones del Consejo sobre la posición en materia de ciberseguridad que piden a la Comisión que presente una propuesta para un Fondo de Emergencia de Ciberseguridad. Los Estados miembros deberían aprovechar plenamente estas oportunidades de conformidad con los requisitos aplicables.

(26) La red mundial submarina de cable de datos y comunicaciones electrónicas es fundamental para la conectividad mundial y dentro de la UE. Dada la gran longitud de estos cables y su instalación en el fondo marino, la vigilancia visual subacuática de la mayoría de las secciones de cable es extremadamente difícil. La jurisdicción

---

19 Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, relativa a un Mecanismo de Protección Civil de la Unión (DO L 347 de 20.12.2013, p. 924).

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf.

compartida y otras cuestiones jurisdiccionales relacionadas con estos cables constituyen una cuestión particular para la cooperación europea e internacional en materia de protección y recuperación de infraestructuras. Por ello, es necesario completar las evaluaciones de riesgos en curso y previstas relativas a las infraestructuras digitales y físicas que sustentan los servicios digitales con evaluaciones de riesgos específicas y opciones para medidas de mitigación con respecto a los cables submarinos. Por consiguiente, la Comisión llevará a cabo estudios con este fin y compartirá sus conclusiones con los Estados miembros.

(27) Los sectores prioritarios definidos en la presente Recomendación de la energía y el transporte también pueden verse afectados por los riesgos relacionados con la infraestructura digital. Tal repercusión puede darse, por ejemplo, en relación con las tecnologías energéticas que incorporan componentes digitales. La seguridad de las cadenas de suministro asociadas es importante para la continuidad de la prestación de servicios esenciales y para el control estratégico de infraestructuras críticas gestionadas por entidades del sector de la energía. Estas circunstancias deberían tenerse en cuenta a la hora de adoptar medidas para mejorar la resiliencia de las entidades que explotan infraestructuras críticas de conformidad con la presente Recomendación.

(28) La importancia creciente de las infraestructuras espaciales y de los servicios espaciales para las actividades relacionadas con la seguridad hace que sea esencial garantizar la resiliencia y la protección de los recursos y servicios espaciales de la Unión dentro de esta, pero también en el marco de la presente Recomendación, es preciso hacer un uso más estructurado de los datos y servicios espaciales proporcionados por los sistemas y programas espaciales para la vigilancia y la protección de las infraestructuras críticas en otros sectores. La futura estrategia espacial de la UE para la seguridad y la defensa propondrá medidas adecuadas a este respecto, que deben tenerse en cuenta a la hora de aplicar la presente Recomendación.

(29) La cooperación internacional también es necesaria para abordar eficazmente los riesgos para la resiliencia de las entidades que explotan infraestructuras críticas, ya sea en la Unión, en terceros países pertinentes o en aguas internacionales. Por lo tanto, debe invitarse a los Estados miembros a cooperar con la Comisión y el Alto Representante para adoptar determinadas medidas a tal efecto, entendiéndose que tales medidas solo deben adoptarse de conformidad con sus respectivas funciones y responsabilidades recogidas en el Derecho de la Unión, en particular las disposiciones de los Tratados de la Unión relativas a las relaciones exteriores.

(30) Como se estableció en la Comunicación «Contribución de la Comisión a la defensa europea»[21], en apoyo de la Brújula Estratégica para la Seguridad y la Defensa para una Unión Europea que protege a sus ciudadanos, valores e intereses y que contribuye a la paz y seguridad internacional[22], la Comisión evaluará las líneas de base de la resiliencia híbrida en cooperación con el Alto Representante y los Estados miembros, identificando las deficiencias y necesidades así como las medidas para abordarlas de aquí a 2023. Esta iniciativa debe servir de base para el trabajo que se realice en el marco de la presente Recomendación, contribuyendo a reforzar el intercambio de información y la coordinación de las acciones, en relación con un mayor refuerzo de la resiliencia, también de las infraestructuras críticas.

---

21 com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu).

22 Consejo de la Unión Europea, ref. 7371/22, de 21 de marzo de 2022.

(31) La Estrategia de Seguridad Marítima de la Unión Europea de 2014 y su plan de acción instaban a una mayor protección de las infraestructuras marítimas críticas, entre ellas, las submarinas, y, en particular del transporte marítimo y las infraestructuras de energía y comunicación, entre otras cosas mediante un mejor conocimiento del ámbito marítimo, a través de la mejora de la interoperabilidad y la simplificación del intercambio de información (obligatorio y voluntario). En este momento, la Estrategia y el plan de acción están siendo actualizados e incluirán medidas reforzadas destinadas a proteger las infraestructuras marítimas críticas. Estas medidas deben completar y enriquecer la presente Recomendación.

(32) Los Estados miembros deben tener en cuenta todo el potencial del programa de investigación sobre seguridad de la Unión, y en particular aprovechar su prioridad específica en materia de infraestructuras críticas, en concreto en el marco de los programas financiados por el Fondo de Seguridad Interior, así como otras posibles oportunidades de financiación a escala de la Unión, especialmente el Fondo Europeo de Desarrollo Regional, en la medida en que las medidas específicas cumplan sus requisitos de admisibilidad. REPowerEU también puede ofrecer posibilidades de financiación para la resiliencia. Todo uso de las oportunidades que ofrece la financiación de la Unión debe producirse de conformidad con los requisitos jurídicos aplicables.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

CAPÍTULO I: OBJETIVO, ÁMBITO DE APLICACIÓN Y DETERMINACIÓN DE PRIORIDADES

(1) La presente Recomendación invita a los Estados miembros a adoptar medidas urgentes y eficaces y a cooperar de forma leal, eficiente, solidaria y coordinada entre sí, con la Comisión y con otras autoridades públicas pertinentes, así como con las entidades afectadas, a fin de mejorar la resiliencia de las infraestructuras críticas utilizadas para la prestación de servicios esenciales en el mercado interior.

(2) Las medidas establecidas en la presente Recomendación se refieren a las infraestructuras designadas por un Estado miembro como infraestructuras críticas, también como infraestructuras críticas europeas.

(3) Al aplicar la presente Recomendación, debe darse prioridad a la mejora de la resiliencia, con respecto a los riesgos de origen humano, de las entidades que operan en los sectores de la energía, la infraestructura digital, el transporte y el espacio, y de las infraestructuras críticas que dichas entidades gestionan y que tienen importancia transfronteriza.

CAPÍTULO II: MEJORAR LA PREPARACIÓN

Acciones a escala de los Estados miembros

(4) Se invita a los Estados miembros a que lleven a cabo o actualicen evaluaciones de riesgos relativas a la resiliencia de las entidades que explotan infraestructuras críticas europeas designadas en los sectores del transporte y la energía en virtud de la Directiva 2008/114/CE y a que busquen la cooperación mutua en dichas evaluaciones y en las medidas de mejora de la resiliencia que de ellas se deriven, según proceda y de conformidad con dicha Directiva.

(5) Asimismo, y con el fin de lograr un alto nivel de resiliencia de las entidades que explotan infraestructuras críticas, los Estados miembros deben acelerar los trabajos

preparatorios para transponer y aplicar lo antes posible la nueva Directiva REC, y para ello deberán:

(a) agilizar la adopción o actualización de estrategias nacionales para la mejora de la resiliencia de las entidades que explotan infraestructuras críticas con el fin de responder a la amenaza actual. Las partes pertinentes de dicha estrategia deben comunicarse a la Comisión;

(b) realizar o actualizar evaluaciones de riesgos en consonancia con la naturaleza cambiante de las amenazas actuales, en lo relativo a la resiliencia de las entidades que explotan infraestructuras críticas en sectores pertinentes más allá de la energía, la infraestructura digital, el sector del transporte y el espacial, y cuando sea posible en aquellos sectores incluidos en el ámbito de aplicación de la nueva Directiva REC, a saber, la banca, las infraestructuras de los mercados financieros, la infraestructura digital, la salud, el agua potable, las aguas residuales, las administraciones públicas, el espacio y la producción, transformación y distribución de alimentos, teniendo en cuenta la posible naturaleza híbrida de las amenazas, incluidos los efectos en cascada y los efectos del cambio climático;

(c) informar a la Comisión sobre los tipos de riesgos detectados por sector y subsector y sobre los resultados de las evaluaciones de riesgos, lo cual puede hacerse utilizando un modelo común de notificación elaborado por la Comisión en cooperación con los Estados miembros;

(d) acelerar el proceso de identificación y designación de las entidades críticas, dando prioridad a las entidades críticas que:

(a) utilicen infraestructuras críticas que estén conectadas físicamente entre dos o más Estados miembros;

(b) formen parte de estructuras corporativas que estén conectadas o vinculadas a entidades críticas de otros Estados miembros;

(c) hayan sido identificadas como tal en un Estado miembro y presten servicios esenciales en seis o más Estados miembros o a seis o más Estados miembros y, por tanto, tengan una especial importancia para Europa, e informen de ello a la Comisión;

(d) cooperar entre sí, en particular en lo que respecta a las entidades críticas y los servicios esenciales y las infraestructuras críticas de importancia transfronteriza, en particular, celebrando consultas entre sí para los fines indicados en el punto 5, letra d) e informándose mutuamente en caso de un incidente con un efecto transfronterizo significativo o potencialmente significativo y manteniendo al mismo tiempo informada a la Comisión como corresponda;

(e) aumentar el apoyo a las entidades críticas designadas con el fin de mejorar su resiliencia, lo que puede incluir el suministro de materiales y metodologías, la organización de ejercicios para poner a prueba su resistencia y proporcionar asesoramiento y formación a su personal, así como facilitar controles de antecedentes personales de las personas con funciones sensibles, de conformidad con la legislación nacional y de la Unión, como parte de las medidas de gestión de la seguridad de los empleados por parte de las entidades críticas;

(f) agilizar la designación o la creación de un punto de contacto único en el seno de la autoridad competente para ejercer una función de enlace a fin de garantizar la cooperación transfronteriza relativa a la resiliencia de las entidades que explotan

infraestructuras críticas con los puntos de contacto únicos de otros Estados miembros.

(6) Se anima a los Estados miembros a que lleven a cabo pruebas de resistencia de las entidades que explotan infraestructuras críticas. En particular se les invita a que avancen en su preparación y la de las entidades afectadas en el sector de la energía y lleven a cabo pruebas de resistencia en este sector, siguiendo, cuando sea posible, principios comúnmente acordados a escala de la Unión, al tiempo que garantizan una comunicación eficaz con las entidades de que se trate. Las pruebas de resistencia en otros sectores prioritarios como la infraestructura digital, el transporte y el espacio, si fuera necesario, podrán considerarse posteriormente teniendo debidamente en cuenta las inspecciones en los subsectores aéreo y marítimo con arreglo al Derecho de la Unión, y teniendo en cuenta también las disposiciones pertinentes de la legislación sectorial.

(7) Se invita a los Estados miembros a que cooperen, cuando proceda y de conformidad con el Derecho de la Unión, con terceros países pertinentes en lo que respecta a la resiliencia de las entidades que explotan infraestructuras críticas con importancia transfronteriza.

(8) Asimismo, se invita a los Estados miembros a que hagan uso, de conformidad con los requisitos aplicables, del potencial de la Unión y de las oportunidades de financiación a nivel nacional para la mejora de la resiliencia de las entidades que explotan infraestructuras críticas en la Unión, por ejemplo, en las redes transeuropeas, frente a toda la gama de amenazas significativas, en particular en el marco de los programas financiados por el Fondo de Seguridad Interior y el Fondo Europeo de Desarrollo Regional, siempre que se cumplan los respectivos criterios de admisibilidad, y el Mecanismo «Conectar Europa», incluidas disposiciones sobre la defensa contra el cambio climático. La financiación del Mecanismo de Protección Civil de la Unión también puede utilizarse con este fin, de conformidad con los requisitos aplicables, en particular para proyectos relacionados con evaluaciones de riesgo, planes o estudios de inversión, creación de capacidades o mejora de la base de conocimientos. REPowerEU también puede ofrecer posibilidades de financiación para la resiliencia.

(9) En cuanto a la infraestructura de redes y comunicaciones en la Unión, el Grupo de cooperación SRI debe, actuando de conformidad con el artículo 11 de la Directiva (UE) 2016/1148, y posteriormente con el artículo 14 de la Directiva SRI 2, acelerar su labor actual sobre una evaluación específica de riesgos y presentar las primeras recomendaciones a principios de 2023. Esta labor debe realizarse garantizando la coherencia y la complementariedad con la labor realizada por el Grupo de cooperación SRI en su línea de trabajo sobre la seguridad de la cadena de suministro de tecnologías de la información y la comunicación, así como por otros grupos pertinentes, como el Grupo de Resiliencia de las Entidades Críticas que se creará en virtud de la nueva Directiva REC y el Foro de Supervisión que se establecerá con arreglo al nuevo Reglamento sobre la resiliencia operativa digital del sector financiero[23].

(10) Se invita al Grupo de cooperación SRI, que debe desempeñar sus funciones de conformidad con el artículo 11 de la Directiva (UE) 2016/1148 y posteriormente con el artículo 14 de la Directiva SRI 2, a que, con el apoyo de la Comisión y de la

[23] COM(2020) 595 final.

ENISA, dé prioridad a su trabajo sobre la seguridad del sector de la infraestructura digital y el sector espacial, en particular, por ejemplo, mediante la preparación de orientaciones políticas y metodologías y medidas de gestión de riesgos de ciberseguridad basadas en un enfoque que abarque todos los riesgos en relación con los cables submarinos de comunicación, anticipándose a la entrada en vigor de la Directiva SRI 2, así como a su labor sobre la elaboración de orientaciones para las medidas de gestión de riesgos de ciberseguridad destinadas a los operadores del sector espacial con el fin de aumentar la resiliencia de las infraestructuras terrestres que dan apoyo a la prestación de servicios espaciales.

(11) Los Estados miembros deben hacer pleno uso de los servicios de preparación en materia de ciberseguridad ofrecidos en el programa de apoyo a corto plazo de la Comisión ejecutado junto con la ENISA, en particular las pruebas de penetración para detectar puntos vulnerables, y, en este contexto, se les anima a dar prioridad a las entidades que explotan infraestructuras críticas en los sectores de la energía, la infraestructura digital y el transporte.

(12) Es urgente que los Estados miembros logren la aplicación de las medidas recomendadas en el conjunto de instrumentos de la UE sobre ciberseguridad de las redes 5G[24]. Los Estados miembros que aún no hayan impuesto restricciones a los proveedores de alto riesgo deben hacerlo sin más demora, teniendo en cuenta que toda pérdida de tiempo puede aumentar la vulnerabilidad de las redes en la Unión. Asimismo, deben reforzar la protección física y no física de las partes críticas y sensibles de las redes 5G, también mediante estrictos controles de acceso. Además, los Estados miembros, en cooperación con la Comisión, deben evaluar la necesidad de medidas complementarias, incluidos requisitos jurídicamente vinculantes a escala de la Unión, a fin de garantizar un nivel coherente de seguridad y resiliencia de las redes 5G.

(13) Los Estados miembros deben aplicar lo antes posible el próximo código de red para los aspectos de ciberseguridad de los flujos transfronterizos de electricidad, basándose en la experiencia adquirida con la aplicación de la Directiva SRI y las correspondientes orientaciones elaboradas por el Grupo de cooperación SRI, en particular, su documento de referencia sobre medidas de seguridad para operadores de servicios esenciales.

(14) Los Estados miembros deben impulsar la utilización de Galileo o Copernicus para la vigilancia y compartir la información pertinente entre los expertos convocados de conformidad con el punto 15. Debe hacerse un buen uso de las capacidades que ofrece la comunicación gubernamental por satélite de la Unión (Govsatcom) del Programa Espacial de la Unión, para seguimiento de las infraestructuras críticas y apoyo a la respuesta a las crisis.

Acciones a escala de la Unión

(15) La Comisión pretende reforzar la cooperación entre los expertos de los Estados miembros para contribuir a mejorar la resiliencia física no cibernética de las entidades que explotan infraestructuras críticas, en particular:

(a) preparando el desarrollo y la promoción de herramientas comunes para ayudar a los Estados miembros a mejorar dicha resiliencia, incluidas metodologías y escenarios de riesgo.

[24] 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf.

(b) respaldando la elaboración de principios comunes sobre la realización de las pruebas de resistencia a que se refiere el punto 6 por parte de los Estados miembros, comenzando por las pruebas que se centran en los riesgos provocados por el hombre en el sector de la energía y posteriormente en otros sectores clave, como la infraestructura digital, el sector del transporte y el espacial; abordando otros riesgos y peligros significativos; así como, cuando proceda, apoyando y asesorando sobre la realización de dichas pruebas de resistencia.

(c) ofreciendo una plataforma segura para recopilar, hacer inventario y compartir las mejores prácticas, las lecciones aprendidas de las experiencias nacionales y otra información relacionada con la resiliencia, también sobre la realización de estas pruebas de resistencia, y traduciendo sus resultados en protocolos y planes de contingencia.

El trabajo de estos expertos debe prestar especial atención a las dependencias intersectoriales y a las entidades que explotan infraestructuras críticas con relevancia transfronteriza, y debe tener continuación en el Grupo de Resiliencia de las Entidades Críticas una vez establecido.

(16) Los Estados miembros deben participar plenamente en la cooperación reforzada a que se refiere el punto 15, entre otras cosas, designando puntos de contacto con los conocimientos pertinentes y compartiendo experiencias sobre las metodologías utilizadas para las pruebas de resistencia y los protocolos y planes de contingencia desarrollados a partir de ellas. El intercambio de información debe preservar la confidencialidad de la información y la seguridad y los intereses comerciales de las entidades críticas, al tiempo que se respeta la seguridad de los Estados miembros. Ello no implica facilitar información cuya divulgación sea contraria a los intereses esenciales de los Estados miembros en materia de seguridad nacional, seguridad pública o defensa.

(17) La Comisión respaldará a los Estados miembros facilitando manuales y directrices, por ejemplo, mediante la elaboración de un manual sobre la protección de las infraestructuras críticas y los espacios públicos contra los sistemas de aeronaves no tripuladas, y herramientas para la evaluación de riesgos. Se invita al SEAE, en particular a través del Centro de Inteligencia y de Situación de la UE y de su Célula de Fusión contra las Amenazas Híbridas, a realizar sesiones informativas sobre las amenazas a las infraestructuras críticas en la UE con el fin de mejorar el conocimiento de la situación.

(18) La Comisión respaldará la adopción de los resultados de los proyectos sobre la resiliencia de las entidades que explotan infraestructuras críticas financiados en el marco de los programas de investigación e innovación de la Unión. La Comisión tiene la intención de aumentar, dentro del presupuesto asignado a Horizonte Europa en el marco financiero plurianual 2021-2027, la financiación destinada a dicha resiliencia. Esto debería permitir abordar los retos actuales y futuros en este ámbito, como la defensa de las infraestructuras críticas contra el cambio climático, sin perjuicio de la financiación de otros fondos de investigación e innovación relacionados con la seguridad civil en el marco de Horizonte Europa. La Comisión también redoblará sus esfuerzos para difundir los resultados de los proyectos de investigación pertinentes financiados por la Unión.

(19) Se invita al Grupo de cooperación SRI, en colaboración con la Comisión y el Alto Representante, de conformidad con sus respectivas funciones y responsabilidades en virtud del Derecho de la Unión, a intensificar el trabajo con las correspondientes

redes y organismos civiles y militares en la realización de evaluaciones de riesgos y la elaboración de escenarios de riesgo de ciberseguridad centrándose inicialmente en las infraestructuras del sector de la energía, las comunicaciones, el transporte y el sector espacial y en las interdependencias entre sectores y Estados miembros. Este ejercicio debe tener en cuenta los riesgos conexos para las infraestructuras físicas de las que dependen estos sectores. Las evaluaciones de riesgos y los escenarios deben realizarse de forma periódica y basarse en las evaluaciones de riesgos existentes o previstos en estos sectores y complementarlas evitando la duplicación, así como servir de base para los debates sobre cómo puede fortalecerse la resiliencia general de las entidades que explotan infraestructuras críticas y abordarse sus puntos vulnerables.

(20) La Comisión acelerará sus actividades de apoyo a la preparación de los Estados miembros y la respuesta a los incidentes de ciberseguridad a gran escala y, en particular:

(a) llevará a cabo, como complemento de las evaluaciones de riesgos en el contexto de la seguridad de las redes y de la información, un estudio exhaustivo que haga inventario de la infraestructura de cable submarino que conecta a los Estados miembros y a Europa a escala mundial, incluida su cartografía, sus capacidades y duplicaciones, sus puntos vulnerables, los riesgos para la disponibilidad del servicio y la mitigación de riesgos. Las conclusiones deben compartirse con los Estados miembros.

(b) apoyará la preparación de la respuesta de los Estados miembros y las instituciones, órganos y organismos de la UE (IOUE) a incidentes de ciberseguridad a gran escala.

(21) La Comisión intensificará los trabajos relacionados con las medidas anticipatorias de cara al futuro también en el marco del Mecanismo de Protección Civil de la Unión, en colaboración con los Estados miembros en virtud de los artículos 6 y 10 de la Decisión 1313/2013/UE, y en forma de planes de contingencia para apoyar la preparación operativa del Centro de Coordinación de la Repuesta a Emergencias.

En particular, la Comisión emprenderá las siguientes actividades:

(a) seguirá trabajando en el Centro de Coordinación de la Respuesta a Emergencias sobre anticipación y prevención intersectorial, preparación y planificación de respuestas a fin de anticiparse y prepararse para interrupciones en la prestación de servicios esenciales por parte de entidades que explotan infraestructuras críticas;

(b) aumentará la inversión en enfoques preventivos y en la preparación de la población en caso de que se produzcan tales interrupciones, con especial atención a los agentes químicos, biológicos, radiológicos y nucleares y explosivos o a otras amenazas emergentes de origen humano;

(c) reforzará el intercambio de conocimientos y mejores prácticas y mejorará el diseño y la realización de actividades de desarrollo de capacidades, como cursos y ejercicios de formación con las entidades que explotan infraestructuras críticas, haciendo uso de las estructuras y los conocimientos especializados existentes, por ejemplo, la Red de Conocimientos sobre Protección Civil de la Unión.

(22) La Comisión fomentará el uso de los recursos de vigilancia de la UE (Copernicus y Galileo) para ayudar a los Estados miembros en la vigilancia de infraestructuras críticas y, cuando proceda, a sus vecinos inmediatos, y para respaldar otras opciones de vigilancia previstas en el Programa Espacial de la Unión.

(23) Cuando sea pertinente y, de conformidad con sus respectivos mandatos, se invita a las agencias de la Unión y a otros órganos pertinentes a que presten apoyo en cuestiones relacionadas con la resiliencia de las entidades que explotan infraestructuras críticas, en particular, de la siguiente manera:

(a) a Europol en la recopilación de información, el análisis criminal y apoyo a la investigación en acciones policiales transfronterizas;

(b) a la Agencia Europea de Seguridad Marítima (AESM) en cuestiones relacionadas con la seguridad y la protección del sector marítimo en la Unión, incluidos los servicios de vigilancia marítima para asuntos relacionados con la seguridad y protección marítimas;

(c) a la Agencia de la Unión Europea para el Programa Espacial (EUSPA) en lo que respecta a las actividades en el marco del programa espacial de la Unión;

(d) a la ENISA en lo relativo a las actividades relacionadas con la ciberseguridad.

CAPÍTULO III: MEJORAR LA RESPUESTA

Acciones a escala de los Estados miembros

(24) Los Estados miembros deben:

(a) coordinar su respuesta y mantener la perspectiva general de la respuesta intersectorial a las perturbaciones importantes en la prestación de servicios esenciales por parte las entidades que explotan infraestructuras críticas en el marco del mecanismo de respuesta a las crisis del Consejo (Dispositivo de la UE de Respuesta Política Integrada a las Crisis – IPCR) en lo que se refiere a las infraestructuras críticas con relevancia transfronteriza, del plan rector sobre incidentes y crisis de ciberseguridad a gran escala o en el marco de una respuesta coordinada de la UE a las campañas híbridas, en caso de una campaña híbrida;

(b) aumentar el intercambio de información dentro del Mecanismo de Protección Civil de la Unión, con el fin de mejorar la alerta temprana y coordinar su respuesta bajo dicho Mecanismo en caso de que se produzcan tales perturbaciones, garantizando así una reacción más rápida propiciada por la Unión cuando sea necesario;

(c) mejorar su preparación para responder a través del Mecanismo de Protección Civil de la Unión a tales perturbaciones significativas, en particular cuando sea probable que tengan implicaciones transfronterizas o incluso paneuropeas importantes, así como intersectoriales;

(d) colaborar con la Comisión para seguir desarrollando las capacidades de respuesta pertinentes en la Reserva Europea de Protección Civil y rescEU;

(e) invitar a las entidades que explotan infraestructuras críticas y a las correspondientes autoridades nacionales a mejorar la capacidad de dichas entidades para restablecer rápidamente el funcionamiento básico de los servicios esenciales que prestan;

(f) garantizar que, cuando sea necesario reconstruir infraestructuras críticas, la infraestructura reconstruida sea resiliente con respecto a toda la gama de riesgos significativos que puedan afectarle, incluso en escenarios climáticos adversos.

(25) Se invita a los Estados miembros a acelerar los trabajos preparatorios para la transposición y aplicación de la Directiva SRI 2, comenzando de inmediato a mejorar las capacidades de los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT), teniendo en cuenta las nuevas tareas de los CSIRT, así como el

aumento del número de entidades de nuevos sectores, actualizando con rapidez sus estrategias de ciberseguridad y adoptando lo antes posible planes nacionales de respuesta a incidentes de ciberseguridad y crisis.

Acciones a escala de la Unión

(26) La respuesta a las perturbaciones importantes en la prestación de servicios esenciales por parte de las entidades que explotan infraestructuras críticas debe coordinarse entre los expertos de los Estados miembros en lo que se refiere a la resiliencia de dichas entidades y las respuestas a tales perturbaciones. Los conocimientos adquiridos a este respecto pueden contribuir a los trabajos del mecanismo de respuesta a las crisis del Consejo (IPCR).

(27) La Comisión colaborará estrechamente con los Estados miembros para seguir desarrollando capacidades desplegables de respuesta a emergencias, incluidos expertos y reservas de rescEU en el marco del MPCU, con vistas a mejorar la preparación operativa para abordar los efectos inmediatos e indirectos de perturbaciones importantes en la prestación de servicios esenciales por parte de las entidades que explotan infraestructuras críticas.

(28) Teniendo en cuenta la evolución del panorama de riesgos y en cooperación con los Estados miembros, la Comisión, en el contexto del MPCU:

(a) analizará y probará continuamente la adecuación y la preparación operativa de la capacidad de respuesta existente;

(b) revisará periódicamente la posible necesidad de desarrollar nuevas capacidades de respuesta a escala de la UE a través de rescEU;

(c) seguirá intensificando la colaboración intersectorial para garantizar una respuesta adecuada a escala de la UE y organizará ejercicios periódicos para poner a prueba dicha colaboración;

(d) seguirá desarrollando el CECRE como centro de crisis intersectorial a escala de la UE para la coordinación de la ayuda a los Estados miembros afectados.

(29) La Comisión, en cooperación con el Alto Representante, en consulta con los Estados miembros y con el apoyo de las agencias pertinentes de la Unión, elaborará un plan rector sobre incidentes y crisis en las infraestructuras críticas que describa y establezca los objetivos y modos de cooperación entre los Estados miembros y las instituciones, órganos, oficinas y agencias de la UE en respuesta a incidentes en infraestructuras críticas, en particular cuando estos impliquen perturbaciones significativas de la prestación de servicios esenciales para el mercado interior. Este plan rector debe hacer uso del Dispositivo de Respuesta Política Integrada a las Crisis (Dispositivo RPIC) para la coordinación de la respuesta.

(30) La Comisión trabajará con las partes interesadas y los expertos sobre posibles medidas de recuperación de incidentes en relación con la infraestructura de cables submarinos, que se presentarán junto con el inventario a que se refiere el punto 20, letra a), y seguirá elaborando planes de contingencia y escenarios de riesgo y trabajando sobre la resiliencia de la Unión ante catástrofes en el marco del Mecanismo de Protección Civil de la Unión.

CAPÍTULO IV: COOPERACIÓN INTERNACIONAL

(31) La Comisión y el Alto Representante apoyarán, cuando proceda y de conformidad con sus respectivas funciones y responsabilidades en virtud del Derecho de la Unión, a países socios para que mejoren la resiliencia de las entidades que explotan infraestructuras críticas en su territorio.

(32) La Comisión y el Alto Representante, en consonancia con sus respectivas funciones y responsabilidades en virtud del Derecho de la Unión, reforzarán la coordinación con la OTAN en materia de resiliencia de las infraestructuras críticas a través del diálogo estructurado UE-OTAN sobre resiliencia y establecerán un grupo de trabajo a tal efecto.

(33) Se invita a los Estados miembros a que contribuyan, en colaboración con la Comisión y el Alto Representante, al desarrollo y aplicación acelerados del conjunto de instrumentos de la UE contra las amenazas híbridas y las directrices de ejecución a que se refieren las conclusiones del Consejo sobre un marco para una respuesta coordinada de la UE a las campañas híbridas[25] y posteriormente a utilizarlos, con el fin de dar pleno efecto al marco para una respuesta coordinada de la UE a las campañas híbridas, en particular cuando consideren y preparen respuestas globales y coordinadas de la UE a las campañas híbridas y a las amenazas híbridas, incluidas las dirigidas contra entidades que explotan infraestructuras críticas.

(34) La Comisión considerará la participación de representantes de terceros países cuando sea adecuado y pertinente en el marco de la cooperación y el intercambio de información entre expertos de los Estados miembros en el ámbito de la resiliencia de las entidades que explotan infraestructuras críticas.

[…]

Hecho en Estrasburgo, el

Por el Consejo
El Presidente

[25] *Council conclusions on a Framework for a coordinated EU response to hybrid campaigns - Consilium (europa.eu)* [«Conclusiones del Consejo sobre un marco para una respuesta coordinada de la UE a las campañas híbridas», comunicado de prensa en inglés].